

# **Zugriff auf Websites mit SSL- Überprüfung blockiert**

Version 2.0



## Einleitung

Es scheint ein anhaltendes Problem mit der Zertifikatskette einer Stammzertifizierungsstelle (ISRG Root X1) zu geben. Dieses Problem betrifft alle Anbieter von SSL-Inspektionsprodukten, unabhängig davon Full-Inspektion oder Zertifikats Inspektion verwendet wird.



**Dieser Issue wird mit dem Release von FortiOS 6.2.10 und 6.4.8 behoben (siehe Release Notes > Resolved Issues)**

### Es besteht folgender Workaround (Stand 05.10.21):

Das *Certificate Bundle* (Version 1.28), welches die *Expired Certificates* ersetzt, ist neu auf FortiGuard erhältlich, und wird im Rahmen geplanter FortiGuard-Updates automatisch heruntergeladen.

Um dies zu validieren, ist folgender CLI-Befehl zu verwenden:

#### Konfiguration über die CLI

```
# diagnose autoupdate versions | grep -A5 '^Cert'

Certificate Bundle
-----
Version: 1.00028
```

Um das *Certificate Bundle* manuell upzudaten, ist folgender CLI-Befehl zu verwenden:

#### Konfiguration über die CLI

```
# execute update-now
```

Sobald das *Certificate Bundle* upgedatet wird, ist der Workaround anwendbar. Um sicherzustellen, dass das *Expired Root CA* nicht mehr verwendet wird, ist *DNS Blackholing* notwendig, welches FortiGate den Zugang zu *apps.identrust.com* blockiert.

Folgend ein **Beispiel** einer möglichen Konfiguration:

#### Konfiguration über die CLI

```
config system dns-database
edit "1"
set domain "identrust.com"
set authoritative disable
config dns-entry
edit 1
set hostname "apps"
set ip 127.0.0.1
next
end
next
end
```



\*Hinweis: Sobald apps.identrust.com keine Expired CA Certificates mehr sendet, kann die Konfiguration entfernt werden  
\*Hinweis: Mittels Teil-Befehl "set authoritative disable" werden andere FQDNs (z.B. commercial.ocsp.identrust.com) weiterhin resolved

Sobald das oben-erwähnte *DNS Blackholing* aktiviert wird, können folgende (vorher getätigte) Änderungen wieder rückgängig gemacht werden:

- 1) Von **Proxy** zu **Flow Inspection**
- 2) Zwischenzeitliches Erlauben von **Expired Certificates**

Mehr Details zu den oberen Schritte findet man unter folgendem Link:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD53305>

-> "Technical Tip: Expiring Let's Encrypt Certificates"

Wichtig: Falls das Problem weiterhin auftaucht, muss eventuell noch der IPS und WAD Cache gelehrt werden (siehe Details im oben-erwähnten KB-Artikel/Link)

Weitere, generelle Informationen findet man unter folgendem Link:

<https://www.fortinet.com/blog/psirt-blogs/fortinet-and-expiring-lets-encrypt-certificates>